Athena7:
Assessing Technical Controls/Backups
Against Real-Time Threat Actor Tactics

ATHENA 7
A CONVERSANT GROUP COMPANY

Would Your Backups Survive a Ransomware Attack? Data Shows, Most Don't.

Threat actors today are more innovative and tenacious than ever—but they are not attacking your policies or your compliance frameworks. They are attacking your technical controls including backups. Will they succeed? Can they move laterally within your environment? Are all critical systems configured properly, or are there gaps in your controls that threat actors may find? You don't have to guess. A technical controls assessment by Athena7 looks at your infrastructure the way an attacker would. Athena7 uses proprietary, real-time threat actor behavior gleaned from our sister company Fenix24, which is on the front lines of ransomware attacks every day. Athena7 experts put that front-line knowledge to work as they "shoulder surf" your critical controls and configurations for vulnerabilities attackers are most likely to target. We will then provide you with an actionable, prioritized roadmap to ensure you have the knowledge necessary in hardening your infrastructure and security against real-world threats.

RANSOMWARE BACKUP & RESILIENCY

Know the SAFETY & RECOVERABILITY of Your BACKUPS

ACTIONABLE TECHNICAL DEFENSE PLAN

Probes POLICIES, PROCESSES, and TECHNICAL CONTROLS

CUSTOMIZED ASSESSMENTS

Built around YOUR SPECIFIC AREAS OF CONCERN

Assessing Technical Controls/Backups details on reverse

> These guys are **my "go to"**: **responsive, technologically deep**, always there when I need them. **I really get the white glove treatment from them!**
>
> — AVI SOLOMON, CISSP, RUMBERGER KIRK

1-877-313-1388
www.athena7.com | **Inquire@athena7.com**

ATHENA7
A CONVERSANT GROUP COMPANY

The Athena7 Assessments: Reverse Engineered to Tell You in Real-time What Threat Actors Will Do if They Gain Access

RANSOMWARE BACKUP AND RESILIENCY: In this assessment, our team will evaluate the safety and recoverability of your backups against a ransomware attack. It focuses on your ability to restore operations in a timely fashion from backups, so you can resume operations without succumbing to attacker demands.

ACTIONABLE TECHNICAL DEFENSE PLAN (ATDP): The ATDP builds on the RBRA but expands the scope to include policies, process, and additional technical controls including password vaulting, network segmentation, and perimeter controls. Athena7 experts will provide you with a plan for remediation on a risk prioritization scale in each assessment.

CUSTOMIZED ASSESSMENTS BUILT AROUND YOUR ORGANIZATION'S NEEDS: Have specific needs or areas of concern? The Athena7 team can scope an assessment catered to your needs. Customized assessments have included: remote access performance (such as Citrix configurations), ATM networks, cloud environments, and more.

Why Athena7?

Unlike other assessment companies, **ATHENA7** doesn't focus on often-outdated frameworks, insurance requirements, or vendor compliance. We go where the threat actors go: your controls and configurations, the true sources of vulnerability hackers are probing constantly. And we do so with the real-world knowledge of current threat actor behavior. The insights from Fenix24 ensure that we know the cyberterrorists' most current playbooks and put them to work in securing your organization so you can evolve your defenses before they become obsolete.

1-877-313-1388
www.athena7.com | Inquire@athena7.com